Informations-säkerhetspolicy för KlickData AB

Stockholm 2021-05-21 Version 2.05

Informationssäkerhetspolicy för KlickData AB

Syfte

Säkerhetspolicyn definierar ramen för hanteringen av informationssäkerhet i KlickData AB (nedan kallat KDAB). Vidare är också syftet att definiera arbetet med informationssäkerheten för KDAB:s kunder data.

Validitet

Säkerhetspolicyn gäller alla anställda i KDAB och hela tillgången till KDAB:s informationssystem. Detta gäller också de data som kunder har eller använder i hela eller delar av KDAB:s system och tjänster.

Förutom anställda vid KDAB gäller policyn också konsulter, partners och underkonsulter som i någon form arbetar med system som tillhandahålls till KDAB:s kunder och användare. En särskild lista med dessa personer samt vilken tillgång till data som givits upprättas och underhålls löpande med noteringar om vilken(a) data/program som konsult har tillgång till.

Mål

- KDAB arbetar aktivt med hanteringen av informationssäkerhet i syfte att säkra tillgänglighet, system och data i alla delar av hanteringen.

- KDAB strävar efter att följa ISO 27001: 2013 / ISO27002: 2013 och motsvarande egna interna säkerhets- och managementstrukturer.

- KDAB använder ett riskbaserat tillvägagångssätt där skyddsnivån och dess kostnad måste baseras på affärsrisken och konsekvensbedömningen som måste utföras årligen som ett minimum.

- En IT-säkerhetshandbok måste utarbetas och kontinuerligt uppdateras. Denna handbok ska innehålla beskrivningar av genomförda åtgärder när det gäller informationssäkerhet och hänvisningar till relevanta policyer, riktlinjer och förfaranden.

- KDAB syftar till att följa relevant lagstiftning, inklusive t.ex. GDPR.

- KDAB har för avsikt att följa avtal med externa parter, inklusive databehandlingsavtal och därmed relaterade säkerhetsrutiner.

- KDAB strävar efter att utarbeta ett årligt uttalande, dvs. ISAE3402, ISAE3000, ISO-certifikat eller likvärdigt internt utarbetad rapport.

- Denna informationssäkerhetspolicy ska ses över årligen i samband med KDAB:s årliga säkerhetsgenomgång.

Organisering och ansvar

- Styrelsen har det yttersta ansvaret för informationssäkerheten i KDAB.

- Ledningen ansvarar för ledningsprinciperna och delegerar specifika ansvarsområden för skyddsåtgärder, inklusive ägande av informationssystem. Äganderätten ställs in för varje kritiskt informationssystem. Ägaren fastställer hur skyddsåtgärder används och hanteras i enlighet med säkerhetspolicyn.

- IT-avdelningen konsulterar, koordinerar, kontrollerar och rapporterar om säkerhetens status. IT-avdelningen utarbetar även riktlinjer och rutiner.

- Den enskilda medarbetaren (likaså konsult, partner etc) är ansvarig för att följa säkerhetspolicyn och informeras om den i ”IT-användningspolicyn”. Alla medarbetare genomgår en utbildning om KDAB:s säkerhetspolicy och säkerhetsarbete. Externa konsulter eller partners genomgår också utbildningen och ges KDAB:s certifiering att arbeta i våra system.

Undantag

Undantag från KDAB:s informationssäkerhetspolicy och riktlinjer godkänns av IT-avdelningen baserat på riktlinjerna från ledningen.

Rapportering

- IT-avdelningen informerar ledningen om alla relevanta säkerhetsintrång och informerar löpande om aktuell hotbild och omfattning av relevanta attackförsök.

- Undantagsstatus ingår i IT-avdelningens årsredovisning till ledningen.

- Ledningen granskar säkerhetsstatus årligen och rapporterar till styrelsen efteråt.

Överträdelse

Avsiktligt brott och missbruk rapporteras av IT-avdelningen till ledningen och den närmaste myndigheten med huvudansvar.

Överträdelse av informationssäkerhetspolicyn och stödjande riktlinjer kan leda till konsekvenser för arbetsrätten eller kontraktsbrott (för konsult/partner).